PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-344442**

(43)Date of publication of application : **29.11.2002**

(51)Int.Cl. **H04L 9/28**

G06F 12/00

G06F 12/14

G09C 1/00

H04L 9/08

(21)Application number : **2001-147911**

(22)Date of filing : **17.05.2001**

(71)Applicant : **DAINIPPON PRINTING CO LTD**

(72)Inventor : **YANO YOSHIHIRO**

OSHIMA NAOYUKI

(54) DATA TRANSMITTER AND DATA RECEIVER AND COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide communication equipment, capable of transmitting and receiving desired data with higher security property.

SOLUTION: Two IC cards 40-1 and 40-2, and 40-3 and 40-4, respectively held

by a user and a manager, are mounted at both a transmission side and a reception side so that divided pattern tables, key tables, and enciphered pattern tables stored to be divided in the respective two IC cards can be formed as a complete table, and that the following data communication processing can be properly executed. Under that condition, data to be transmitted are connected and then divided by a data dividing part 13, and added with electronic signatures by an electronic signature part 14, and added with dummy files by a dummy file adding part 15, and added with dummy data by a dummy data adding part 16, and enciphered by an enciphering part 17, and transmitted by a transmitting part 18. At the reception side, the reverse processing is executed, so that the original data file can be restored.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The store interface means which has been arranged at the position and which communicates with the store with which key data were memorized, and reads the key data concerned, A file division means to divide the data file for transmission and to generate two or more division data files, The data source which has an encryption means to encipher alternatively using said key data, and a transmitting means to transmit said two or more of said division data files enciphered alternatively, to said two or more generated division data files.

[Claim 2] Said transmitting means is the data source according to claim 1 with which it has further the electronic office expert stage which performs electronic signature using said read key data to said two or more of said division data files enciphered alternatively, and said electronic signature was made and which transmits said two or more of said division data files enciphered alternatively.

[Claim 3] Said electronic office expert stage is the data source according to claim 2 which performs said electronic signature by enciphering to two steps through said store interface means using the 2nd key data read from the 1st key data and 2nd store which were read from the 1st store.

[Claim 4] It is equipment which the user of the data source concerned owns said 1st store substantially, and memorizes the 1st [based on the authority of the user concerned / said] key data. Said 2nd store It is equipment which the manager of the data source concerned owns substantially and memorizes the 2nd [based on the authority of the manager concerned / said] key data. Said electronic office expert stage The data source according to claim 3 which performs said electronic signature by performing 1st encryption using the 1st [based on said user's authority / said] key data, and performing 2nd encryption using the 2nd [based on said manager's authority / said] key data.

[Claim 5] It is the data source according to claim 1 to 4 which has further the file consolidation means which unifies two or more data files for transmission, and is made into the data file of 1, and said file division means divides said combined data file, and generates said two or more division data files.

[Claim 6] Said transmitting means is the data source according to claim 1 to 5 which transmits the file with which it was unified [in / have further the 2nd file consolidation means which unifies two or more division data files divided by said file division means, and / said 2nd file consolidation means].

[Claim 7] A receiving means to receive the transmit data which the data file for transmission was divided, was enciphered respectively alternatively, and was transmitted, The store interface means which has been arranged at the position and which communicates with the store with which key data were memorized, and reads the key data concerned, The data sink which has a decryption means to decrypt alternatively said received transmit data which was enciphered respectively alternatively using said read key data, and a file consolidation means to unify said data decrypted alternatively and to generate the data file for [original / said] transmission.

[Claim 8] It is the data sink according to claim 7 with which said transmit data is data by which electronic signature was further carried out after [said] being enciphered alternatively, it has further an electronic signature inspection means to inspect said electronic signature using said read key data, to said received transmit data by which electronic signature was carried out, and said decryption means decrypts alternatively the transmit data with which inspection of said electronic signature was conducted.

[Claim 9] Said electronic signature inspection means is a data sink according to claim 8 which inspects said electronic signature by decrypting to two steps through said store interface means using the 4th key data read from the 3rd key data and 4th store which were read from the 3rd store.

[Claim 10] It is equipment which the user of the data sink concerned owns said 3rd store substantially, and memorizes the 3rd [based on the authority of the

user concerned / said] key data. Said 4th store It is equipment which the manager of the data sink concerned owns substantially and memorizes the 4th [based on the authority of the manager concerned / said] key data. Said electronic signature inspection means The data sink according to claim 9 which inspects said electronic signature by performing the 1st decryption using the 4th [based on said manager's authority / said] key data, and performing the 2nd decryption using the 3rd [based on said user's authority / said] key data.

[Claim 11] The data file for [of said origin] transmission is a data sink according to claim 7 to 10 which has further a file division means to be the file by which the data file for [two or more] transmission joined together, and was generated, to divide the data file for [of the origin integrated by said file consolidation means / said] transmission, and to generate the data file for [said / two or more] transmission.

[Claim 12] It is the data sink according to claim 7 to 11 which the transmit data received in said receiving means is data with which the data file for [said / which was divided] transmission joined together further, and was generated, it has further the 2nd file division means which divides said received transmit data, and said file-consolidation means unifies said divided data, and generates the data file for [original / said] transmission.

[Claim 13] The portable mold storage interface means which communicates with the portable mold storage which has been arranged at the position, and with which key data were memorized, and reads the key data concerned, A file division means to divide the data file for transmission and to generate two or more division data files, An encryption means to encipher alternatively to said two or more generated division data files using said key data, The data source which has a transmitting means to transmit said two or more of said division data files enciphered alternatively, A receiving means to receive the transmit data which the data file for transmission was divided, was enciphered respectively alternatively, and was transmitted, The portable mold storage interface means which communicates with the portable mold storage which has been arranged at

the position, and with which key data were memorized, and reads the key data concerned, A decryption means to decrypt alternatively said received transmit data which was enciphered respectively alternatively using said read key data, Communication system which has the data sink which has a file consolidation means to unify said data decrypted alternatively and to generate the data file for [original / said] transmission.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data source, the data sink, and communication system for communicating a data file by higher security nature.

[0002]

[Description of the Prior Art] The amount of the information which progress of an information processing technique or communication technology can perform [information] now easily [transmission of the information through a communication network] and efficiently, and is transmitted through a communication network is increasing by leaps and bounds. Although there are various gestalten as such a communication network, its attention is paid to two or more computer systems and the Internet to which the local communication network was connected on a scale of worldwide from the field of the scale and communication link cost, and they are used widely. By the way, the communication link of the data which have various confidentiality between an individual or a company through such a communication network is also performed. And it usually enciphers and the required data of such confidentiality are transmitted. Although a cryptographic key is used for this encryption **** sake,

those who encipher and transmit data need to hold and manage this cryptographic key safely so that it may not lose or reveal.

[0003]

[Problem(s) to be Solved by the Invention] However, with the advance of this encoding technology, the decryption technique is also progressing and it has become the situation which is enciphered and can never be said to be enough [security nature] in a request. For example, when transmitting significant data streams, such as a text, it is known by using general knowledge, such as general structure of a text, a data stream with high operating frequency, and an expression, that a cipher can be decoded comparatively easily. And a code is decoded once, namely, once a cryptographic key or encryption algorithm is decoded, future encryption will become possible [decoding easily like a just addressee], and no confidentiality of data will be held.

[0004] Therefore, decode of a code is more difficult for the purpose of this invention, and is to offer the data source which can transmit desired data by higher security nature. Moreover, other purposes of this invention are by receiving the data transmitted by security nature high such, and decrypting appropriately to offer the data sink which can perform high data reception of security nature. Decode of a code is more more difficult still for other purposes of this invention, and it is in offering the communication device which can transmit desired data and can be received by higher security nature.

[0005]

[Means for Solving the Problem] In order to solve said technical problem, the data source concerning this invention The store interface means which has been arranged at the position and which communicates with the store with which key data were memorized, and reads the key data concerned, A file division means to divide the data file for transmission and to generate two or more division data files, It has an encryption means to encipher alternatively using said key data, and a transmitting means to transmit said two or more of said division data files enciphered alternatively, to said two or more generated division data files.

[0006] Having further the electronic office expert stage which performs electronic signature using said read key data suitably to said two or more of said division data files enciphered alternatively, said transmitting means transmits said two or more division data files enciphered by said selection target by which said electronic signature was made. Moreover, said electronic office expert stage performs said electronic signature by enciphering to two steps through said store interface means suitably using the 2nd key data read from the 1st key data and 2nd store which were read from the 1st store.

[0007] The user of the data source concerned owns said 1st store substantially still more suitably. It is equipment which memorizes the 1st [based on the authority of the user concerned / said] key data. Said 2nd storage It is equipment which the manager of the data source concerned owns substantially and memorizes the 2nd [based on the authority of the manager concerned / said] key data. Said electronic office expert stage Said electronic signature is performed by performing 1st encryption using the 1st [based on said user's authority / said] key data, and performing 2nd encryption using the 2nd [based on said manager's authority / said] key data.

[0008] Moreover, it has further the file consolidation means which unifies two or more data files for transmission, and is suitably made into the data file of 1, and said file division means divides said combined data file, and generates said two or more division data files. Moreover, it has further the 2nd file consolidation means which unifies specifically two or more division data files divided by said file division means, and said transmitting means transmits the file integrated in said 2nd file consolidation means.

[0009] Moreover, a receiving means to receive the transmit data which the data file for transmission was divided, and the data sink concerning this invention was enciphered respectively alternatively, and was transmitted, The store interface means which has been arranged at the position and which communicates with the store with which key data were memorized, and reads the key data concerned, It has a decryption means to decrypt alternatively said received

transmit data which was enciphered respectively alternatively using said read key data, and a file consolidation means to unify said data decrypted alternatively and to generate the data file for [original / said] transmission.

[0010] Suitably, said transmit data is data by which electronic signature was further carried out after [said] being enciphered alternatively, and has further an electronic signature inspection means to inspect said electronic signature using said read key data, to said received transmit data by which electronic signature was carried out, and said decryption means decrypts alternatively the transmit data with which inspection of said electronic signature was conducted. Moreover, said electronic signature inspection means inspects said electronic signature by decrypting to two steps through said store interface means suitably using the 4th key data read from the 3rd key data and 4th store which were read from the 3rd store.

[0011] The user of the data sink concerned owns said 3rd store substantially still more suitably. It is equipment which memorizes the 3rd [based on the authority of the user concerned / said] key data. Said 4th storage It is equipment which the manager of the data sink concerned owns substantially and memorizes the 4th [based on the authority of the manager concerned / said] key data. Said electronic signature inspection means Said electronic signature is inspected by performing the 1st decryption using the 4th [based on said manager's authority / said] key data, and performing the 2nd decryption using the 3rd [based on said user's authority / said] key data.

[0012] Moreover, suitably, the data file for [of said origin] transmission is a file by which the data file for [two or more] transmission joined together, and was generated, divides the data file for [of the origin integrated by said file consolidation means / said] transmission, and has further a file division means to generate the data file for [said / two or more] transmission. Moreover, specifically, it is data with which the data file for [said / which was divided] transmission joined together further, and the transmit data received in said receiving means was generated, said file consolidation means unifies said

divided data by having further the 2nd file division means which divides said received transmit data, and the data file for [original / said] transmission is generated.

[0013] Moreover, the portable mold storage interface means which the communication system concerning this invention communicates with the portable mold storage which has been arranged at the position, and with which key data were memorized, and reads the key data concerned, A file division means to divide the data file for transmission and to generate two or more division data files, An encryption means to encipher alternatively to said two or more generated division data files using said key data, The data source which has a transmitting means to transmit said two or more of said division data files enciphered alternatively, A receiving means to receive the transmit data which the data file for transmission was divided, was enciphered respectively alternatively, and was transmitted, The portable mold storage interface means which communicates with the portable mold storage which has been arranged at the position, and with which key data were memorized, and reads the key data concerned, A decryption means to decrypt alternatively said received transmit data which was enciphered respectively alternatively using said read key data, Said data decrypted alternatively are unified and it has the data sink which has a file consolidation means to generate the data file for [original / said] transmission.

[0014]

[Embodiment of the Invention] The gestalt of 1 operation of this invention is explained with reference to drawing 1 - drawing 9 . Drawing 1 is drawing having shown roughly the whole communication system 1 configuration of the gestalt of this operation. Drawing 2 is the block diagram of communication system 1 showing especially the configuration of a sending set 10 and a receiving set 30 in a detail. As shown in drawing 1 , communication system 1 is the configuration that the sending set 10 and the receiving set 30 were connected through the transmission line 20. And a desired data file can be transmitted and received now

by equipping a sending set 10 and a receiving set 30 with IC card 40-1 which the user and manager of equipment hold respectively, 40-2 and 40-3, and 40-4.

[0015] First, the configuration and function of each part of the communication system 1 are explained. First, IC card 40-1 to 40-4 of each user of the transmitting side and receiving side with which a sending set 10 and a receiving set 30 are equipped, and a manager is explained. Each IC card-i (i=1-4) memorizes setting data, a division pattern table, an encryption pattern table, and a key table respectively.

[0016] Setting data are the information for specifying owners, such as a RSA public key of the user of each ID of the user of cardholder ID, a cardholder name, a password, a user flag, a manager flag, a transmitting side, and a receiving side, and a manager and a name, a cardholder's RSA private key, a cardholder's RSA public key, a corresponding receiving side, or a transmitting side, and a manager, a corresponding manager, the user of a receiving side, and a manager. In addition, a user flag is the flag which shows that the owner of an IC card is a user, and a manager flag is a flag which shows that the owner of an IC card is a manager.

[0017] A division pattern table is a table on which two or more storage of the division pattern which specified the division approach at the time of dividing the data file for transmission was carried out. This division pattern table is respectively divided into two sheets' IC card 40-1 of the each user and manager of a transmitting side and a receiving side, 40-2 and IC card 40-3, and 40-4, and is memorized. That is, by unifying respectively IC card 40-1 of two sheets, 40-2 or IC card 40-3, and the table data of 40-4, table data are memorized by each IC card 40-i so that one division pattern table may be constituted. In addition, IC card, a transmitting side and a receiving side, 40-1 of two sheets each, 40-2 and IC card 40-3, and each division pattern table memorized by 40-4 are the same tables.

[0018] An encryption pattern table is a table on which two or more storage of the data which specified the cipher system at the time of enciphering the data file for

transmission was carried out. This encryption pattern table is respectively divided into two sheets' IC card 40-1 of the each user and manager of a transmitting side and a receiving side, 40-2 and IC card 40-3, and 40-4, and is memorized. That is, by unifying respectively IC card 40-1 of two sheets, 40-2 or IC card 40-3, and the table data of 40-4, table data are memorized by each IC card 40-i so that one encryption pattern table may be constituted. In addition, IC card, a transmitting side and a receiving side, 40-1 of two sheets each, 40-2 and IC card 40-3, and each encryption pattern table memorized by 40-4 are the same tables.

[0019] the cryptographic key used when a key table performs encryption and electronic signature in a transmitting side -- moreover, the decode key used when conducting decryption and inspection of electronic signature in a receiving side is the table by which each two or more storage is carried out. This key table is also respectively divided into two sheets' IC card 40-1 of the each user and manager of a transmitting side and a receiving side, 40-2 and IC card 40-3, and 40-4, and is memorized. That is, by unifying respectively IC card 40-1 of two sheets, 40-2 or IC card 40-3, and the table data of 40-4, table data are memorized by each IC card 40-i so that one key table may be constituted.

[0020] And the manager whose user (operator) who actually operates a sending set 10 is usually the user's superior official about 1st IC card 40-1 for users in a transmitting side and whose IC card 40-1 to 40-4 with which such each data was memorized is the person in charge of the processing in a sending set 10 holds respectively 2nd IC card 40-2 for managers. Moreover, in a receiving side, the manager the user who actually operates a receiving set 30 is usually the user's superior official about 3rd IC card 40-3 for users, and is [manager] a person in charge of the processing in a receiving set 30 holds respectively 4th IC card 40-4 for managers.

[0021] Next, a sending set 10 is explained. A sending set 10 combines and divides the data file of the request for transmission suitably, and adds a dummy file and dummy data. Furthermore, a sending set 10 adds electronic signature, enciphers, and is transmitted to a receiving set 30 through a transmission line 20.

A sending set 10 has the IC card read station 11, the user / manager transmission-and-reception side specification section 12, the data division section 13, the electronic signature section 14, the dummy file adjunct 15, the dummy data adjunct 16, the encryption section 17, and the transmitting section 18, as shown in drawing 2 .

[0022] The IC card read station 11 reads the information on the division pattern table used by the division processing and encryption processing after IC card 40-1 of coincidence or the user by whom sequential wearing is done, and a manager's IC card 40-2, an encryption pattern table, a key table, etc. First the IC card read station 11 from therefore, a user's IC card 40-1 with which it was equipped and a manager's IC card 40-2 Cardholder ID, the cardholder name which are memorized as setting data, Each ID, a name, etc. of the user of a password, a user flag, a manager flag, a transmitting side as shown in drawing 3 , and a receiving side, and a manager, The information for specifying an owner, a corresponding manager, the user of a receiving side, and a manager is read, and is outputted to the user / manager transmission-and-reception side specification section 12 mentioned later.

[0023] When it is detected in a user / manager transmission-and-reception side specification section 12 that the owner of user's IC card 40-1 and a manager's IC card 40-2 is the user and manager of the proper sending set 10 As shown in drawing 4 , the IC card read station 11 next, from 40 to IC card [of a user] 40-1 and IC card of manager 2 each The information on the division pattern table mentioned above, an encryption pattern table, a key table and the transmitting-side manager RSA private key of setting data, a transmitting-side user RSA private key, a receiving-side manager's RSA public key, and a receiving-side user's RSA public key etc. is read. And an encryption pattern table and a key table are outputted to the encryption section 17, and the data which need setting data, such as key information, are outputted for the read division pattern table to the data division section 13 at the electronic signature section 14.

[0024] Based on the information on each ID of the user of cardholder ID and the

cardholder name which are inputted from the IC card read station 11, a password user flag, a manager flag, a transmitting side, and a receiving side, and a manager, a name, etc., the operator who equipped the sending set 10 with a user's IC card 40-1 and a manager's IC card 40-2 detects whether you are the user and manager of the proper sending set 10, and a user / manager transmission-and-reception side specification section 12 notifies a detection result to the IC card read station 11.

[0025] The data division section 13 combines two or more data files for [which was inputted] transmission, and generates one connection file. And one united connection file is divided into two or more momentary division files based on the division pattern table read from a user's IC card 40-1 and a manager's IC card 40-2, and it outputs to the dummy file adjunct 15. As mentioned above, two or more conventions of the division pattern with which the distribution place file for every cutting tool of each data of a data file as shown in drawing 5 (A) is indicated are carried out at the division pattern table. The data division section 13 divides into three files the file combined with one based on the division pattern which chose the division pattern of arbitration and was chosen from two or more of these division patterns, as shown in drawing 5 (B). Moreover, in this case, the data division section 13 calculates the hash value of the file name of the connection file combined previously, and outputs it to the electronic signature section 14.

[0026] The hash value of the file name of the connection file which combined the data file for [into which the electronic signature section 14 is inputted from the data division section 13] transmission, It is based on ID of each user of the initial cryptographic key number created by the encryption section 17 mentioned later, a transmitting side, and a receiving side, and a manager, and the information on a name. The electronic signature data which created and created electronic signature data using the transmitting-side manager RSA private key inputted by the IC card read station 11, the transmitting-side user RSA private key, a receiving-side manager's RSA public key, and a receiving-side user's RSA public

key are outputted to the dummy file adjunct 15.
[0027] Drawing 6 is drawing showing the structure of electronic signature data. The hash value storing section is a field which stores the data which carried out RSA cipher processing of the hash value of the file name of the connection file which combined the data file for [which is inputted from the data division section 13] transmission using a transmitting-side user's RSA private key, and carried out RSA cipher processing further using a receiving-side manager's RSA public key. The key storing section is a field which stores the data which carried out RSA cipher processing of the initial cryptographic key number created by the encryption section 17 mentioned later using a receiving-side user's (operator) RSA public key, and carried out RSA cipher processing further using a transmitting-side manager's RSA private key. Moreover, the signature path storing section is a field which stores the data which carried out DES encryption of ID and name of each user of a transmitting side and a receiving side, and a manager. Based on the data of the hash value storing section mentioned above and the key storing section, the predetermined Ruhr generates the DES cryptographic key used in the case of this DES encryption.
[0028] As one or more dummy files which are files of the contents unrelated to a division file temporarily generated in the data division section 13 are generated and it is shown in drawing 7 , the dummy file adjunct 15 is added to two or more of the momentary division files inputted from the data division section 13, and is outputted to the dummy data adjunct 16. At this time, the dummy file adjunct 15 writes in the number of the division pattern table which generated or was used for the dummy file in the data division section 13, the initial value of the DES encryption processing used in the encryption section 17, and the electronic signature data generated in the electronic signature section 14.
[0029] To a division file, the dummy data adjunct 16 adds dummy data to the any one, plurality, or its all alternatively temporarily which is inputted from the dummy file adjunct 15, as shown in drawing 8 . And a division file and the dummy file added by the dummy file adjunct 15 are outputted to the encryption section 17

temporarily [these]. In addition, dummy data is added to each file here so that the data size of each file may become the multiple which is 8 bytes.

[0030] The encryption section 17 carries out encryption processing of a division file and the dummy file temporarily [when dummy data was added alternatively] which is inputted from the dummy data adjunct 16 using the cryptographic key which generated and generated the cryptographic key based on the encryption pattern table and key table which were read in the IC card read station 11 from a user's IC card 40-1 and a manager's IC card 40-2, and outputs them to the transmitting section 18. Moreover, the encryption section 17 combines the hash value of the file name of the dummy file generated by the electronic signature data and the dummy file adjunct 15 which were generated in the electronic signature section 14, generates the control file containing this, and outputs it to the transmitting section 18.

[0031] As shown in drawing 9 (A), two or more cipher systems are specified on the encryption pattern table read from a user's IC card 40-1 and a manager's IC card 40-2. Moreover, as similarly shown in drawing 9 (A), two or more cryptographic keys are registered into the key table read from a user's IC card 40-1 and a manager's IC card 40-2. Based on the cryptographic key which chose cipher systems, such as Triple DES, and chose and chose the cryptographic key of arbitration from two or more of these cipher systems from two or more of these cryptographic keys, the encryption section 17 enciphers, as shown in drawing 9 (B).

[0032] The transmitting section 18 transmits the enciphered division file which is inputted from the encryption section 17, a dummy file, and a control file to a receiving set 30 through a transmission line 20. By the sending set 10 of such a configuration, the data file for [desired] transmission is sent out to a transmission line 20.

[0033] A transmission line 20 is a transmission line of the arbitration which connects a sending set 10 and a receiving set 30, and is the Internet in the gestalt of this operation.

[0034] Next, the receiving set 30 of communication system 1 is explained. A receiving set 30 receives the data which various processings which were mentioned above in the sending set 10 were performed, and were transmitted through the transmission line 20, processes integration of a decryption, removal of a dummy file, removal of dummy data, and data, division, etc., and restores the original data file. A receiving set 30 has a receive section 31, the IC card read station 32, the user / manager transmission-and-reception side specification section 33, the dummy file removal section 34, the electronic signature section 35, the decryption section 36, the dummy data removal section 37, and the data integration section 38, as shown in drawing 2 .

[0035] A receive section 31 receives the data transmitted through the transmission line 20 from the sending set 10, i.e., the enciphered division file, a dummy file, and a control file, and outputs to the dummy file removal section 34.

[0036] The IC card read station 32 reads the information on the division pattern table used by the decryption processing and integrated processing after IC card 40-3 of coincidence or the user by whom sequential wearing is done, and a manager's IC card 40-4, an encryption pattern table, a key table, etc. First the IC card read station 32 from therefore, a user's IC card 40-3 with which it was equipped and a manager's IC card 40-4 Cardholder ID, the cardholder name which are memorized as setting data, Each ID, a name, etc. of the user of a password, a user flag, a manager flag, a transmitting side, and a receiving side, and a manager, The information for specifying an owner, a corresponding manager, the user of a receiving side, and a manager is read, and it outputs to a user / manager transmission-and-reception side specification section 33.

[0037] If it is detected in a user / manager transmission-and-reception side specification section 33 that the owner of user's IC card 40-3 and a manager's IC card 40-4 is the user and manager of the proper receiving set 30, the IC card read station 32 will read next the information on the division pattern table mentioned above, an encryption pattern table, a key table, etc. from 40 to IC card [of a user] 40-3 and IC card of manager 4 each. And an encryption pattern table

and a key table are outputted to the decryption section 36, and the data which need setting data, such as key information, are outputted for the read division pattern table to the data integration section 38 at the electronic signature section 35.

[0038] Based on the information on each ID of the user of cardholder ID and the cardholder name which are inputted from the IC card read station 32, a password, a user flag, a manager flag, a transmitting side, and a receiving side, and a manager, a name, etc., the operator who equipped the receiving set 30 with a user's IC card 40-3 and a manager's IC card 40-4 detects whether you are the user and manager of the proper receiving set 30, and a user / manager transmission-and-reception side specification section 33 notifies a detection result to the IC card read station 32.

[0039] The dummy file removal section 34 analyzes the control file inputted by the receive section 31, reads the hash value of the file name of the dummy file stored in the control file, and specifies a dummy file from each data file inputted by the receive section 31. And after specifying a dummy file, the dummy file and the division file which remained are outputted to the decryption section 36.

[0040] By performing opposite processing of the electronic signature section 14 mentioned above one by one, the electronic signature section 35 performs decryption processing of the electronic signature data inputted from the decryption section 36, and extracts the hash value of a connection file, initial cryptographic key data, and signature path data. And the hash value of the extracted connection file is passed through initial cryptographic key data decryption section 36 to the data integration section 38, and signature path data are outputted to a user / manager transmission-and-reception side specification section 33.

[0041] The decryption section 36 decrypts the dummy file and division file which are inputted from the dummy file removal section 34. The decryption section 36 asks for a decode key based on the hash value of a control file first, decrypts a dummy file using this, and generates a dummy file temporarily. Next, from a

dummy file, the decryption section 36 extracts the initial value of a DES decode key, generates a DES decode key based on this, and decrypts a division file temporarily which was decrypted. Moreover, from a dummy file, the decryption section 36 extracts a division pattern number, and outputs it to the data integration section 38 temporarily which was decrypted. Moreover, the decryption section 36 combines the contents of a dummy file and the control file temporarily which was decrypted, generates electronic signature data, and outputs them to the electronic signature section 35.

[0042] The dummy data removal section 37 removes dummy data from a division file temporarily which is inputted from the decryption section 36, and outputs it to the data integration section 38.

[0043] The data integration section 38 unifies a division file based on a division pattern, and generates one connection file temporarily which was generated by the dummy data removal section 37. And one generated connection file is divided and two or more original data files are restored. By the above, a receiving set 30 restores and outputs two or more original data files from the received data.

[0044] In addition, a sending set 10 and a receiving set 30 are realized by carrying the software which realizes the function of each configuration section of the IC card read station 11 - the transmitting section 18 and a receive section 31 - the data integration section 38 for an IC card drive to general-purpose computer equipments, such as one set or a personal computer which has two sets and has the means of communications in which the node of arbitration and a communication link are possible through a transmission line 20.

[0045] Next, actuation of communication system 1 is explained. If two or more data files for transmission are inputted into a sending set 10 and preparations of transmission are made, as for a transmitting-side user, a transmitting-side manager will equip a sending set 10 with transmitting-side manager IC card 40-2 for transmitting-side user IC card 40-1 respectively. In a sending set 10, the IC card read station 11 attests the owner of IC card 40-1 and IC card 40-2 first. Consequently, if IC card 40-1 and the owner of 40-2 are proper next, a user /

manager transmission-and-reception side specification section 52 will check the relation between a transmitting-side user and a transmitting-side manager. And if it is a case also with the proper relation between a user and a manager, from two IC cards 40-1 and 40-2, the IC card read station 51 will read a configuration file, a partial division pattern table, a code pattern table, and a cryptographic key table, and will output them to the electronic signature section 14, the data division section 13, and the encryption section 17 respectively.

[0046] First, two or more data files for [which was inputted] transmission are divided into two or more different momentary division files from the original data file, once it is combined with one file in the data division section 13. At this time, the approach of that division is determined based on the specific division pattern with which two IC cards 40-1 and the division pattern table read from 40-2 were chosen. Next, a dummy file is added in the dummy file adjunct 15, and further, dummy data is added in the dummy data adjunct 16, and it is respectively enciphered in the encryption section 17. This encryption is performed by the specific cipher system chosen from two IC cards 40-1 and the code pattern table read from 40-2 using the specific cryptographic key chosen from two IC cards 40-1 and the key table read from 40-2.

[0047] In addition, in the electronic signature section 14, a dummy file is overlapped on the electronic signature data which electronic signature data were created based on ID of each user of the hash value of the file name of a connection file, an initial cryptographic key number, a transmitting side, and a receiving side, and a manager, and the information on a name, and were created in the dummy file adjunct 15 with a division pattern number and the initial value of encryption processing in this case. And each file and control file which were enciphered are transmitted to a receiving set 30 through a transmission line 20.

[0048] In the receiving set 30, each FARU transmitted in the receive section 31 is received, and it memorizes to the storage in a receiving set 30. And if the user and manager of a receiving side equip a receiving set 30 with IC card 40-3 and 40-4 and acquire authentication like a sending set 10, perusal processing of the

file which received will be started. That is, a dummy file is first specified by the dummy file removal section 34 from the information on a control file. The specified dummy file is decrypted in the decryption section 36, and the electronic signature data on which it was superimposed, a division pattern number, and the initial value of encryption processing are extracted. Next, in the electronic signature section 35, the hash value of a signature path, an initial cryptographic key number, and a connection file is extracted from the extracted signature, and the user and manager by the side of transmission and reception are specified by a user / manager transmission-and-reception side specification section 33 from a signature path.

[0049] Next, in the decryption section 36, with the decode key changed and called for from the initial value and the initial cryptographic key number which were extracted previously, each file which received is decrypted and dummy data is removed in the dummy data removal section 37. And once the they-decrypted file is compounded by one connection file, it is divided into the multiple files for [original] transmission by the data integration section 38, it reverts to two or more original data files, and it is outputted from a receiving set 30.

[0050] Thus, in the communication system 1 of the gestalt of this operation, the data file for transmission was unified and divided, dummy data was added, and the dummy file was added, and it enciphered further and has transmitted. Therefore, compared with the case where it only enciphers, decode is very difficult and can transmit data in the condition that security nature is more high. Moreover, processing of encryption, a decryption, electronic signature, etc. cannot be performed if two persons' IC card, a user and a manager, of two sheets is not used. Therefore, one user can raise security nature compared with the conventional method of performing these processings by his authority.

[0051] In addition, this invention is not restricted to the gestalt of this operation, and arbitrary suitable various alterations are possible for it. For example, it divides, after combining two or more data files for transmission in the data division section 13, and he is trying to transmit the multiple files generated based

on this from the transmitting section 18 in the sending set of the gestalt of operation mentioned above. However, the file divided by doing in this way is unified before transmitting in the transmitting section 18 further, and it collects into one file, and you may make it transmit this. You may join together only in sequence, and it shuffles by a certain approach and you may make it unify the approach of the integration in that case. Moreover, you may make it arrange the integrated section for the file consolidation in the latter part of the encryption section, and may make it arrange it in the preceding paragraph of the encryption section. Moreover, you may make it prepare the division section which once divides the file which received suitably in a receiving set according to such deformation of a sending set. Of course, even if the file for [original] transmission is one, it does not interfere at all, and even if it is such a case, subsequent division, integration, etc. of a file may be performed like the case where there are two or more files.

[0052] Moreover, in the gestalt of operation mentioned above, although proper encryption processing and decryption processing are performed and it is made to perform desired data communication by using the IC card of two sheets, the configuration that only the IC card of one sheet is used may be used. Moreover, it may be made to perform acknowledgement of data communication etc. using the IC card of three or more sheets. Moreover, a contact mold, an adhesion mold, the non-contact mold of the gestalt of an IC card, etc. are good with the gestalt of arbitration. Furthermore, you may make it use the storage of arbitration, such as a magnetic card instead of what is restricted to the so-called IC card, and storage.

[0053] Moreover, the sequence of processings, such as the sequence of processing and the dummy file removal in a receiving set, electronic signature inspection and decryptions, such as data coupling in a sending set, data division, electronic signature, dummy file addition, dummy data addition, and encryption, dummy data removal, data integration, and data division, is not restricted to the gestalt of this operation, and may be changed into arbitration. Moreover, the data concerning the encryption and the decryption which are memorized to an IC card

etc. are good by the data of arbitration. In addition, in the case of the gestalt of operation mentioned above, the configuration of a sending set 10 and a receiving set 30, the method of each encryption, etc. are not restricted, and may be changed into arbitration.

[0054]

[Effect of the Invention] Thus, according to this invention, decode of a code is more difficult and can offer the data source which can transmit desired data by higher security nature. Moreover, the data sink which can perform high data reception of security nature can be offered by receiving the data transmitted by security nature high such, and decrypting appropriately. Furthermore, decode of a code is more difficult and can offer the communication device which can transmit desired data and can be received by higher security nature.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is the block diagram showing the outline of the whole configuration of the communication system of the gestalt of 1 operation of this invention.

[Drawing 2] Drawing 2 is the block diagram showing the configuration of the sending set of the communication system shown in drawing 1 , and a receiving set in a detail.

[Drawing 3] Drawing 3 is drawing showing the condition of reading ID and name of the user by the side of the transmission and reception memorized, and a manager in an IC card in the IC card read station of the sending set shown in drawing 2 .

[Drawing 4] Drawing 4 is drawing showing the condition of reading the division pattern table memorized, an encryption pattern table, a key table, and CDC in an

IC card in the IC card read station of the sending set shown in drawing 2 .

[Drawing 5] Drawing 5 is drawing showing the processing which divides the file for transmission based on the division pattern table in the data division section of the sending set shown in drawing 2 read in the IC card.

[Drawing 6] Drawing 6 is drawing showing the electronic signature data generated by the electronic signature section of the sending set shown in drawing 2 .

[Drawing 7] Drawing 7 is drawing in the dummy file adjunct of the sending set shown in drawing 2 showing the processing which adds a dummy file.

[Drawing 8] Drawing 8 is drawing in the dummy data adjunct of the sending set shown in drawing 2 showing the processing which adds dummy data.

[Drawing 9] Drawing 9 is drawing showing the processing which enciphers the file for transmission based on the encryption pattern table and key table in the encryption section of the sending set shown in drawing 2 which were read in the IC card.

[Description of Notations]

1 -- Communication system

10 -- Sending set

11 -- IC card read station

12 -- A user / manager transmission-and-reception side specification section

13 -- Data division section

14 -- Electronic signature section

15 -- Dummy file adjunct

16 -- Dummy data adjunct

17 -- Encryption section

18 -- Transmitting section

20 -- Transmission line

30 -- Receiving set

31 -- Receive section

32 -- IC card read station

33 -- A user / manager transmission-and-reception side specification section

34 -- Dummy file removal section

35 -- Electronic signature section

36 -- Decryption section

37 -- Dummy data removal section

38 -- Data integration section

40-1 to 40-4 -- IC card